MORRISON | FOERSTER

User tracking: Scope and Implementation ePrivacy Directive Article 5(3)

Email Sender & Provider Coalition
April 3, 2012

Presented By
Karin Retzer

Tracking – The European Framework

- Tracking, analytics, and behavioral advertising are subject to two sets of requirements
  - Amendments to **ePrivacy Directive 2002/58/EC** amended by Directive 2009/136/EC of 25 November 2009 which introduced specific requirements for cookies and similar tracking technologies
  - **Data Protection Directive 1995/46/EC** which provides general rules for processing personal data
- Draft Regulation will replace Data Protection Directive and apply directly to non-European sites processing personal data, provided European EU/EEA residents are monitored or profiled, or to sites providing products or services

Data Protection Directive

- Data Protection Directive was the main vehicle of the EU/EEA data protection regime
- It applies broadly to anyone processing personal data
- Personal data includes any information relating to an identified or identifiable natural person
  - Direct or indirect identification, e.g., by reference to identifying information held by third parties
  - May include IP addresses
  - Location data covered
  - Draft Regulation further broadens definition
- Processing comprises any collection, use, access, transfer, or deletion of personal data

Legitimate Basis

- Data Protection Directive prohibits any processing of personal data unless there is a "legitimate basis"
  - Consent of the individual concerned
    - Specific requirements for sensitive data such as health data
    - Article 29 Working Party Guidelines state that with respect to ad networks, individuals' silence or failure to act can never be considered valid consent
    - Draft Regulation imposes requirement for consent to be "explicit", including through clear affirmative action
  - Contractual necessity
  - Compliance with (local) legal obligations
  - Balance of interest test, marketing not generally covered by balance of intest test

Transfer

- Restrictions on data transfers
  - Transfer means any sharing or accessing of personal data
  - No restrictions for sharing data within the EU/EEA
  - Transfers to non-EU/EEA countries prohibited unless there is adequate protection or narrow exceptions apply
- In certain countries, the local entity must register its processing and/or transfer of personal data with a local data protection authority

Notice, Access and Correction

- **Notice**
  - All individuals should be provided with notice about what data are collected, the purposes for which they will be used, and with whom the data are shared
  - Draft Regulation imposes specific additional requirements

- **Access and Correction**
  - All individuals may request access to their personal data and must have the opportunity to correct information that is incorrect or incomplete
  - Draft Regulation mandates a 30-day response time limit

Security and Data Retention

- Personal data must be kept secure and confidential
- Whenever personal data are processed by service providers there should be a written data processing agreement
- Personal data should not be retained (stored) for longer than is necessary, i.e., the period of time that the personal data serves the purpose for which they were collected (unless legal hold or other applicable law provides otherwise)

The ePrivacy Directive

- The ePrivacy Directive complements the Data Protection Directive and covers cookies and other tracking technologies
- Implementation deadline was May 25, 2011, but some countries still need to implement
- Article 5(3) requires clear and comprehensive notice and consent **where information is stored or accessed on the user's terminal equipment**
- In most countries, the bills or adopted legislation are unclear as to the type of consent

Which Technologies Are Covered?

- Provisions are aimed at browser cookies but may also apply to other tracking technologies that store or access information locally, such as locally stored objects (LSO) or flash cookies, document object model (DOM), advertisement tags, and JavaScript codes that are integral to the functioning of websites or used for online advertising
- Pixel tags/beacons or device fingerprinting that do not drop cookies are not technically covered by Article 5(3) but may be covered by the Data Protection Directive
- Analytics covered in some Member States but exempted by others

WP29 Interpretation

- Article 29 Working Party Opinion on online behavioral advertising adopted June 2010
- Covers only third-party online behavioral advertising (OBA)
  - Tracking of users as they surf the Internet
  - The building of profiles over time, which are later used to provide users with advertising that matches their interests
- Does not cover analytics or contextual or segmented advertising
- Very strict interpretation—notice and opt-in consent required irrespective of whether personal data are collected; IAB/EASA Code of Conduct and Good Practice Principles insufficient

The Position in Germany

- No specific implementation. Cookies covered by general data protection laws, the Federal Data Protection Act and the Telemedia Act
- Düsseldorfer Kreis Opinion issued in November 2009 requires opt-in consent for collection of full IP addresses
- Proposal from Länder representation and political opposition in German Parliament to allow for opt-out and broader exemption; government reluctant to act on proposal

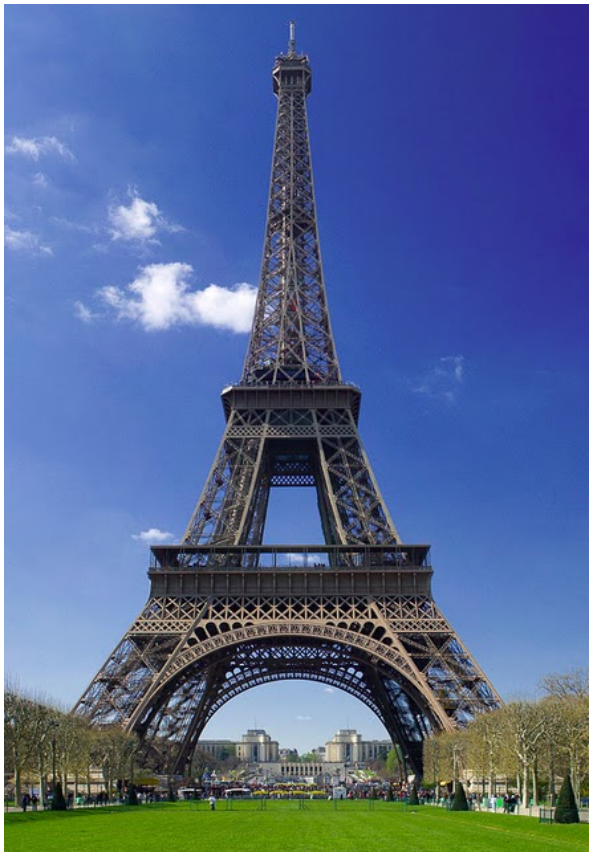
The Position in the UK

- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 in force
- Copies wording of ePrivacy Directive
- ICO guidance updated in December 2011 without major changes
  - Current browser settings that accept cookies by default not sufficient. Businesses should seek consent through other means, depending on how "intrusive" use of cookies may be (cookies policy, header/footer language on the web, icons, etc.)
  - Regulations designed to protect users' privacy wherever information is collected for profiling purposes —Web operators should consider broad intentions of Regulations when using or considering other technologies such as device fingerprinting in place of cookies
- One-year grace period during which new rules will not be enforced, provided there is a "realistic plan" to achieve compliance. Grace period only applies in the UK - ends May 26, 2012

The Position in Ireland

- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 in force
- Regulations apply to all information stored or gathered via cookies, apps, or other situations, irrespective of whether personal data are stored/accessed—analytics exempt
- Prior informed consent required
- Consent can be expressed through browser settings, but not in their current form
- Online policies should be expanded to include full details on cookies
- Policies should be prominently placed, easily accessible, and intelligible to users

The Position in France



- Ordinance No. 2011-1012—amendments to Data Protection Act, Electronic Communications Code, and Consumer Protection Code in force
- Prior informed consent required
- Consent does not have to be opt-in/express—implied or tacit consent suffices, e.g., through browser settings, but not in their current form
- Exemption from notice and consent requirements where cookies are used to facilitate communication or are strictly necessary to deliver service to customer (e.g., cookies used (only) for the delivery of the site or security purposes, language and other local preferences of the user, flash cookies required for the to provide multimedia services)
- CNIL recommends banners in the upper portion of the site, tick-boxes, or floaters

The Position in the Netherlands

- Draft bill amending Telecommunications Act
- Consent must be explicit and limited to specific placement of cookies and other information about which users have been informed
- Goes beyond the ePrivacy Directive and requires web operators to be able to prove that consent has been obtained
- Use of cookies for tracking triggers for and application of general data protection rules
- Government has said consent is not the only legal basis for use of cookies

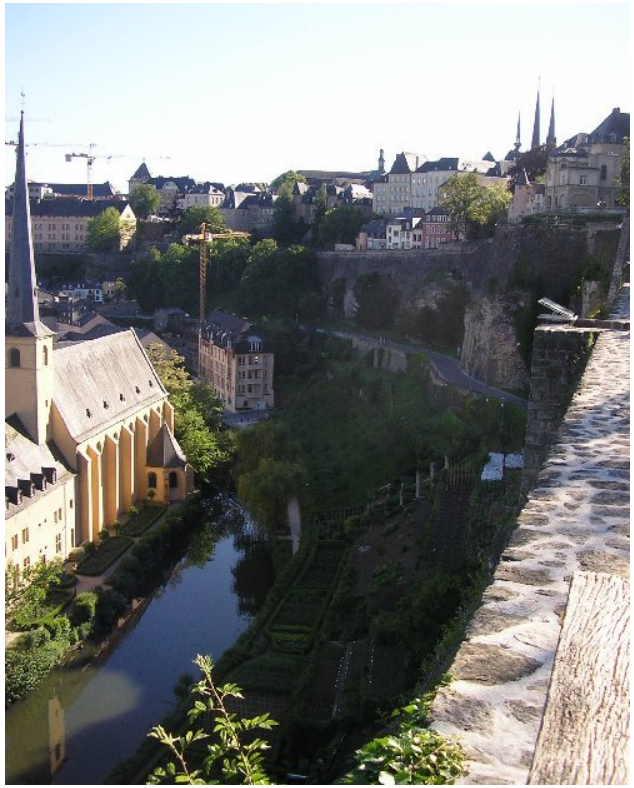
The Position in Finland

- Act on the Protection of Privacy in Electronic Communications in force
- Prior consent required, but can be expressed through current browser settings
- Online policies should be expanded to include full details on cookies
- Policies should be prominently placed, and easily accessible and intelligible to users

The Position in Austria

- Amendment to Telecommunications Act 2003, effective as of November 21, 2011
- *Prior* consent is required not only for the use of cookies but for the collection of all data online by website operators
- Browser settings are a valid method of obtaining consent. It is unclear whether existing default browser settings are sufficient

The Position in Luxembourg



- The Law of July 28, 2011 on the protection of data in the electronic communications sector amends Luxembourg's Modified Law of May 30, 2005 (Protection of data and electronic communications)
- The Law introduces *prior* consent to the use of cookies and similar technologies
- The Law copies the wording of the Directive
- Consent must be prior, informed, and freely given and "where technical possible" appropriate browser settings or other application settings are a valid method of providing consent.
- Provision of information and the method of giving consent should be as user-friendly as possible

The Position in Sweden

- Bill amending the Electronic Communications Act (2003:389) entered into force July 1, 2011
- The Bill directly copies the language of the Directive, although the possibility to use browser settings as a means of obtaining consent is not included in the text, only in legislative materials.
- The provisions do not provide details on whether the required user consent should be opt-in or opt-out, but legislative materials suggest that opt-out through browser settings should generally suffice
- A “question and answer” guide for website owners published June 28 by the Swedish Post and Telecom Agency (“PTS”), does not provide any further clarifications on the type or frequency of consent, and only states that website owners should implement appropriate technical solutions to obtain consent

The Position in Italy

- Implementation legislation currently not in place
- An Italian Community Law 2010 became effective January 17, 2012 and requires that the Italian government adopts a Decree to implement the Directive within three months
- Parliament must adopt the Government Decree within 60 days of it being issued

Consent requirements per country

	Opt-in	Opt-out	Unclear
Adopted Legislation	Germany Lithuania	Czech Republic Estonia	Austria Denmark Finland France Hungary Ireland Latvia Luxembourg Slovakia Sweden UK

Consent requirements per country

	Opt-in	Opt-out	Unclear
Draft Legislation	Cyprus Netherlands	Bulgaria Poland	Belgium Denmark Greece Italy Malta Portugal Spain Romania

Compliance Steps You Can Take Now

- EU/EEA countries still grappling with the implications of new rules—there are no easy answers as to what compliance means or how best to achieve it
- Position likely to develop over the coming months
- Prudent to monitor developments and consider following steps
  - Audit your site, know what types of cookies are set and how information is used
  - Improve transparency
  - Ensure greater user control

Audit Your Site

- Identify what cookies are currently used and for what purposes
- Audit the tags on the web pages that call your servers (and third-party servers) to drop old cookies
- Determine if any exemptions apply
  - **Cookies used to deliver and improve services for users** are most likely to be exempted from the general obligations to provide notice and obtain consent
  - **For all other cookies**, in particular those used for analytics
    - Improve transparency by providing users with clear and transparent notice
    - Ensure greater user control by obtaining user consent

Improve Transparency (1)

- Expand privacy policy to include
  - The types of cookies set
  - Purposes for which data are used, e.g., whether data are combined with log-in data
  - With whom the data are shared
  - How to manage cookies—more explicit references to cookie controls in browser tool menus
  - Exception for session cookies and other cookies "strictly necessary" for specific services explicitly requested by the subscriber or user

Improve Transparency (2)

- Ensure privacy policy is prominently placed
  - Notice must be clear and comprehensive and as user friendly as possible
- Consider notice outside the privacy policy
  - Pop-up may spoil user experience, single pop-up for same activity may suffice
  - Icon or text in web page header/footer leading to enhanced notice regarding analytics
  - Notice when users log in or agree to certain features or settings
  - Help menu

Ensure Greater User Control (1)

- Stronger emphasis on consent
  - ePrivacy Directive does not refer to any specific type of consent as it does in the section on spamming ("*prior explicit consent*")
  - Member States may choose implied consent but mere right to object is insufficient
  - Where "*technically possible and effective*," default browser settings or other applications would be a means to provide consent (Recital 66)

Ensure Greater User Control (2)

- Where possible, obtain opt-in consent
  - Where users register or log in
  - Via highlighted or scrolling headers, footers, or splash screens that must be acknowledged
- Where not possible, consider
  - Prominent opt-out consent
  - Using alternative technologies
- The more granular and affirmative each consent is, the more likely it is to be valid
- Provide the means for more persistent opt-out, e.g., in notices

EU Materials

- **EU Data Protection Directive**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
- **Draft EU General Data Protection Regulation**
  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- **ePrivacy Directive**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF
- **Opinion 2/2010 on online behavioral advertising (WP29)**
  http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

Country-specific Materials

- **UK – ICO guidance on implementation of ePrivacy Directive**
  http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf
- **France – CNIL guidance**
  http://www.cnil.fr/english/news-and-events/news/article/what-the-telecoms-package-changes-for-cookies/
- **Ireland – Data Protection Commissioner's guidance**
  http://www.dataprotection.ie/viewdoc.asp?DocID=1152&ad=1#12